NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Number   Yes   No   Recommended Protective Measures:	Action			otective measure to a different alert level.  BLUE- GUARDED (GENERAL RISK of terrorist attack)
B-1 Disseminate the BLUE advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.  B-2 Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.  Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing surveillance cameras in vulnerable areas.  • Providing a pack-up power source for critical functions.  • Installing an alarm system for critical buildings, coors, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PlO) on appropriate response measures, protective actions, and self help				
B-1 related to the Homeland Security Threat Condition with state agencies/offices and government officials.  Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.  Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate in relation to the current Hom	Number	162	INO	
B-2 Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.  Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Geach department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in	B-1			
B-2 Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.  Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  Issuing employee picture ID badges.  Conducting background checks on employees, if authorized.  Installing surveillance cameras in vulnerable areas.  Providing a back-up power source for critical functions.  Installing an alarm system for critical buildings, doors or offices.  Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate. Coordinate information releases with other government entities, if possible.  Brief Public Information Officer (PlO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate				
B-3 GREEN Advisory. Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Geach department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  Issuing employee picture ID badges.  Conducting background checks on employees, if authorized.  Installing surveillance cameras in vulnerable areas.  Providing a back-up power source for critical functions.  Installing an alarm system for critical buildings, doors or offices.  Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate. Coordinate information releases with other government entities, if possible.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site m				
Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of as sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Con	B-2			· · · · · · · · · · · · · · · · · · ·
B-3				
B-3  Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting back-up power source for critical functions.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / pa				
B-3  Mutual Aid Agreements, etc., as applicable). Each department/agency/office should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate. Coordinate information releases with other government entities, if possible.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to rem				
department/agency/ortnice should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  Issuing employee picture ID badges.  Conducting background checks on employees, if authorized.  Installing surveillance cameras in vulnerable areas.  Providing a back-up power source for critical functions.  Installing an alarm system for critical buildings, doors or offices.  Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to g	D 2			
functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.  Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  Issuing employee picture ID badges.  Conducting background checks on employees, if authorized. Installing surveillance cameras in vulnerable areas. Providing a back-up power source for critical functions. Installing an alarm system for critical buildings, doors or offices. Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature. Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Com	B-3			department/agency/office should be familiar with their assigned
emergency plans and Mutual Aid agreements.				responsibilities according to the plan. Conduct tabletop and
Implement security plans appropriate to the facilities and assets involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information activates. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
involved. Review communications plans and update the call-down procedures as necessary. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include:  • Issuing employee picture ID badges.  • Conducting background checks on employees, if authorized.  • Installing surveillance cameras in vulnerable areas.  • Providing a back-up power source for critical functions.  • Installing an alarm system for critical buildings, doors or offices.  • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.  • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
B-4  B-4  B-4  B-6  B-7  B-7  B-7  B-7  B-7  B-8  B-8  B-8	B-4			
B-4  B-4  B-4  B-4  B-4  B-4  B-4  B-5  B-6  B-6  B-7  B-7  B-7  B-7  B-8  B-8  B-8  B-8				·
B-4  B-4  B-4  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to pereational posterior, as appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate.  B-8  B-8  B-8  Reviewendal Actively support the Neighborhood Watch, Community Emergency Reprose Team (CERT), Community Policing (COP) and Amateur Radio Evaluate information available on public websites that could				J
B-4  B-4  B-4  B-4  B-4  B-5  B-6  B-7  B-7  B-7  B-7  B-8  B-8  B-8  B-8				
B-4  Conducting background checks on employees, if authorized. Installing surveillance cameras in vulnerable areas. Providing a back-up power source for critical functions. Installing an alarm system for critical buildings, doors or offices. Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature. Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
Installing surveillance cameras in vulnerable areas. Providing a back-up power source for critical functions. Installing an alarm system for critical buildings, doors or offices. Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature. Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
Providing a back-up power source for critical functions.     Installing an alarm system for critical buildings, doors or offices.     Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.     Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
Installing an alarm system for critical buildings, doors or offices.     Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.     Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
<ul> <li>Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.</li> <li>Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.</li> <li>Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.</li> <li>Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.</li> <li>Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.</li> <li>Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.</li> <li>Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.</li> </ul>				
from buildings, particularly buildings of a sensitive nature.  Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
B-5  Review and update your organizations critical infrastructure list. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.				
Review and update your organizations critical infrastructure list.  Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-5  Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
Countermeasures required to protect them.  Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could	B-5			
Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) ( <a href="https://www.ares.org/">http://www.ares.org/</a> ) programs.  Evaluate information available on public websites that could				
B-6 specialized response equipment (e.g., HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.  Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10 Evaluate information available on public websites that could	B-6			Check all equipment for operational readiness, fill fuel tanks, check
Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10  Brate				
B-7  measures, protective actions, and self help options appropriate to the Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				command post, generators, etc.), as appropriate.
B-7 Homeland Security Threat Condition. Activate the jurisdiction Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could	B-7			
B-8  Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-9  information releases with other government entities, if possible.  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-8  Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-8  Current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-8 handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10 Evaluate information available on public websites that could	B-8			
report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10  Evaluate information available on public websites that could				
package processing and sorting facility to reduce the threat to government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10  Evaluate information available on public websites that could				
government employees, if situation dictates.  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  B-10  Evaluate information available on public websites that could				
B-9  Actively support the Neighborhood Watch, Community Emergency Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) (http://www.ares.org/) programs.  Evaluate information available on public websites that could				
B-9 Response Team (CERT), Community Policing (COP) and Amateur Radio Emergency Service (ARES) ( <a href="http://www.ares.org/">http://www.ares.org/</a> ) programs.  Evaluate information available on public websites that could				
Emergency Service (ARES) ( <a href="http://www.ares.org/">http://www.ares.org/</a> ) programs.  Evaluate information available on public websites that could	B-9			
R-10 Evaluate information available on public websites that could				
B_	D 40			
	B-10			·